COMPARATIVE REVIEW

Comparing Wares

It was initially intended to use *NetWare 5* as the operating system for this review, but with only a minority of the products offering features specifically for the latest *Novell* platform, and for the sake of speed (the tests run comparatively slowly on the machine used as the test server) *NetWare 4.10* was in fact used for the bulk of testing.

Perhaps the introduction of *NetWare 5* is responsible for the relatively small number of products that were submitted for testing. Quite a few products are currently receiving some sort of facelift, and so only ten developers sent us their wares, one less than in the previous *NetWare* Comparative Review (see *VB*, July 1998 p.11).

Test Procedures

In common with all recent comparatives, various aspects of each scanner's properties were investigated. Detection rates for on-demand scanning have been determined using a test-set consisting of standard, macro and polymorphic viruses. In addition to this, each product has been tested against a virus set aligned to the April 1999 WildList. Given the submission deadline of 30 April (for product shipping) this In the Wild test-set gives us a realistic impression of how well each product copes with the viruses that are known to be prevalent in the real world.

New additions to the WildList since the last comparative include the *Microsoft Office*-infecting O97M/Triplicate.C, W97M/Pri.B and the infamous W97M/Melissa.A. As for all Comparative Reviews, additions were also made to the other test-sets. Making their debuts in the *VB* test-sets this month are {Win32,W97M}/Beast (analysed in last month's *VB*, June 1999 p.6) and the polymorphic file infector Win32/ACG (see p.8 of this issue). For a complete listing of the test-sets used for testing, see the URL listed at the end of this review.

The performance of the on-access (real-time) scanner is fundamental to the usefulness of any anti-virus product. Beside the obvious importance of detection rates, the overhead such a scanner imposes upon the server must also be considered. Irrespective of how good its detection rate is, a scanner that log-jams the server, reducing its performance, is undesirable. Thus the overhead of each of the on-access scanners has been tested, by monitoring the time taken to copy a set of 200 files (100 COM/EXE and 100 OLE2) between directories on the server. By normalizing the results to the average baseline (with no on-access scanner loaded) of 28 seconds, the results presented within this review are expressed in units of time, as well as in terms of percentage overhead.

Perhaps of less importance to the day-to-day running of anti-virus software, the scanning speed of each of the on-demand scanners has also been investigated. For this, two file sets have been used. The first is a 5500 file COM/EXE collection (520 MB), and the second a 373 file OLE2 (DO? and XL?) collection (65.3 MB). These sets are virus-free, and so also provide a false positive test for all the products.

A slight change has been made to the format of the main results tables this month. The detection rates have been calculated as usual, and are expressed in the usual percentage format. However, instead of listing the number of detected samples, the tables now list the number of *missed* samples. The detection rates are also listed beneath each of the product headings (for on-demand scanning unless indicated otherwise). Since detection rates are normalized with respect to the number of samples of each virus, products that miss the same number of samples do not necessarily achieve the same percentage detection rate.

CA InnoculateIT v4.5 (13/04/99)

ItW File	100.0%	Macro	99.7%
ItW File (o/a)	100.0%	Macro (o/a)	99.7%
Standard	99.9%	Polymorphic	96.8%

It appears that the old *InnocuLAN* name badge from the *Cheyenne* days has gone, and as with the rest of the *Computer Associates* range, the product is now adorned with the suffix '*IT*'.

In addition to the server-based virus-scanning component, *InnoculateIT* provides the user with the option to install a centralized management component. Using this, the administrator has full control of deployment, configuration and scanning right across the network.

Anti-virus protection is initiated by simply running the NCF file that is created during installation. The server console is designed with real-time anti-virus protection as its main focus. On-demand scans can be configured and initiated however, and multiple tasks can be created and placed in a job queue.

The first product this time around to detect all the in-the-wild viruses during both on-demand and on-access scanning, *InnoculateIT* maintains the high standard it set in the previous *Windows 98* comparative. Detection elsewhere in the test-sets was equally commendable.

In terms of scanning speed, *InnoculateIT* performs just above average when compared to other products featured in this review. Scan rates of just over 430 KB/sec and 1290 KB/sec were obtained for scanning of the executable and OLE2 files on the hard disk respectively.

On-demand tests	ItW File		Macro		Polymorphic		Standard	
	Missed	%	Missed	%	Missed	%	Missed	%
CA InnoculateIT	0	100.0%	7	99.7%	175	96.8%	1	99.9%
Command AntiVirus	4	99.7%	33	99.2%	173	96.8%	0	100.0%
CA Vet NetWare	20	98.1%	139	95.8%	423	95.8%	3	99.6%
DialogueScience DrWeb	3	99.7%	34	98.8%	107	98.0%	35	95.8%
Kaspersky Lab AVP	3	99.7%	25	99.1%	50	99.2%	3	99.6%
NAI NetShield	16	99.0%	31	99.1%	428	95.8%	0	100.0%
Norman FireBreak	13	98.8%	47	98.5%	174	96.8%	1	99.9%
Proland Protector Plus	77	89.4%	1,626	42.5%	11,095	22.3%	852	32.4%
Sophos Anti-Virus	4	99.7%	43	98.6%	174	96.8%	12	99.5%
Symantec Norton AntiVirus	0	100.0%	13	99.4%	175	96.8%	0	100.0%

The overhead of the on-access scanner is similar to that for the other products, reaching approximately 40% when scanning both incoming and outgoing files.

Command AntiVirus v4.54 SP2 (24/04/99)

ItW File	99.7%	Macro	99.2%
ItW File (o/a)	99.7%	Macro (o/a)	99.0%
Standard	100.0%	Polymorphic	96.8%

An *InstallShield* installation routine is used to copy the necessary server and workstation files to their desired destinations. An option to install *AlertTrack*, an NLM to manage alert notification across a network, is also provided.

Admirably high detection rates across all the test-sets were observed, although complete In the Wild detection was hampered by O97M/Tristate.C-infected *PowerPoint* and *Excel* files. Despite changing the configuration to scan All Files, the *PowerPoint* files were not scanned and so remained undetected.

Configuration of the *F-PROT* virus engine can be achieved either from the server console using the wealth of command line switches that are available, or using an administration utilty at the workstation. Scanning speeds were certainly not quick, even when the tests were repeated with the limits upon the CPU usage removed. Perhaps more relevant to the day to day use of the product though is the overhead the on-access scanner of *Command AntiVirus* imposes. Tests showed only a small overhead (just under 50%) when scanning both incoming and outgoing files.

CA Vet NetWare v9.9.4

ItW File	98.1%	Macro	95.8%
ItW File (o/a)	98.1%	Macro (o/a)	95.6%
Standard	99.6%	Polymorphic	95.8%

Yes, the title is correct. This is the second product from *Computer Associates* this month, thanks to their recent acquisition of the *Vet AntiVirus* products.

Installation of *Vet NetWare* has to be performed from the workstation, and is achieved by running the setup program on the supplied diskettes. Subsequently, configuration and initiation of scans is initiated from either the server console or via RCONSOLE from the workstation. *Vet NetWare* employs configuration sets for saving and loading multiple configurations, which allows up to 16 set-ups to be stored.

One slight annoyance with *Vet NetWare* is that there is no indication of scan progress on the server console, merely a message box stating that a scan is in progress. The detection rates observed were slightly lower than those expected from recent performances by the Australian product, but it should be noted that this is predominantly due to the omission of quite a few file types from the default file extension list.

On-access tests	ItW File		Macro		Polymorphic		Standard	
	Missed	%	Missed	%	Missed	%	Missed	%
CA InnoculateIT	0	100.0%	7	99.7%	176	96.8%	1	99.9%
Command AntiVirus	4	99.7%	45	99.0%	173	96.8%	0	100.0%
CA Vet NetWare	20	98.1%	142	95.6%	423	95.8%	2	99.7%
Kaspersky Lab AVP	17	98.9%	28	99.1%	296	98.2%	12	99.4%
NAI NetShield	16	99.0%	31	99.1%	428	95.8%	0	100.0%
Norman FireBreak	13	98.8%	47	98.5%	174	96.8%	1	99.9%
Sophos Anti-Virus	4	99.7%	43	98.6%	174	96.8%	12	99.5%
Symantec Norton AntiVirus	0	100.0%	13	99.4%	175	96.8%	0	100.0%

As expected, repeating the tests whilst scanning in All Files mode improved the detection rates markedly, although W97M/Pri.B-infected documents were still missed from the In the Wild test-set.

To avoid overloading of the server, *Vet NetWare* employs a fast scan for scheduled and on-access scanning, looking for viruses in files according to the methods used to infect such files. When a scan is started on-demand however, a more thorough full scan method is used, where each byte of every file is scanned. The difference between the two scan methods was only in evidence once, with a sample of Cantando.857, which, interestingly, was missed during the full scan yet detected during a fast scan.

DialogueScience DrWeb v4.06β (30/04/99)

ItW File	99.7%	Macro	98.8%
ItW File (o/a)	n/t	Macro (o/a)	n/t
Standard	95.8%	Polymorphic	98.0%

Installation of *DrWeb for NetWare* (*DWNW*) was a straightforward affair – simply copying the relevant files to the server manually, and then loading the relevant module. In keeping with other *DialogueScience* anti-virus products the interface of *DWNW* is simple and efficient to use if somewhat dated. In its default settings, *DWNW* scans files by extension and content. Thus, if the extension or the content of a file shows it to be either executable or pertaining to *Microsoft Office*, it is examined by the virus engine.

Detection-wise, *DWNW* performed well across all the test-sets. As with other products in this review the virus engine appears to be unfamiliar with the format of *PowerPoint* files, missing O97M/Triplicate.C infected samples. On the positive side, *DWNW* was one of only three products to detect samples of Win32/ACG – a newcomer to the Polymorphic test-set. This was thanks to *DrWeb's* heuristics (enabled by default), which reported 67 out of the 174 samples to be infected with a COM virus. The downside of such keen heuristics was in evidence during the speed tests however, where 19 clean files were flagged as suspicious.

It was not possible to test the performance of the real-time scanner because upon its activation access to all files on the volume (infected or clean) was denied. Discussion with the *DialogueScience* developers suggested that this was a problem assoiated with the LIBUPI patch applied to the *NetWare 4.10* installation. However, reinstalling *DrWeb* onto the server with various combinations of older patches applied did not solve the problem.

Kaspersky Lab AVP v3.0.121 (30/04/99)

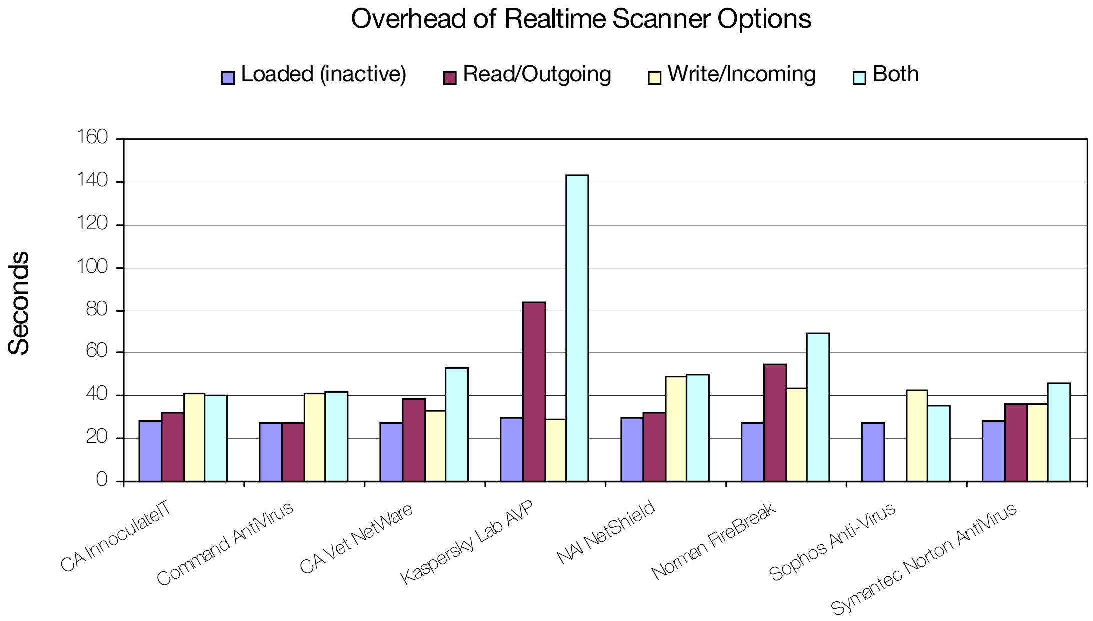
ItW File	99.7%	Macro	99.1%
ItW File (o/a)	98.9%	Macro (o/a)	99.1%
Standard	99.6%	Polymorphic	99.2%

AVP has always had a tradition of high detection rates across the test-sets, and is in the enviable position of having detected 100% of the ItW viruses thrown at it during the last seven comparatives. Such a performance was not to be repeated this time around however, thanks once again to the O97M/Tristate.C-infected *PowerPoint* samples.

Detection rates elsewhere in the test-sets though high, were not as high as have come to be expected of *AVP*. Changing the configuration such that packed files were unpacked during scanning improved the results slighlty - although the bulk of the misses were registered against the infected *PowerPoint* files.

In the last comparative the weakest area of *AVP's* detection was against polymorphic viruses. This seems to have been remedied, and *AVP* correctly detected all but 50 of the ACG samples.

Scanning speed has never been a strong point of *AVP*, and little has changed in this respect – with this product the emphasis has always been upon accurate detection at the expense of speed.



NAI NetShield v4.0.2 SP1 (26/04/99)

ItW File	99.0%	Macro	99.1%
ItW File (o/a)	99.0%	Macro (o/a)	99.1%
Standard	100.0%	Polymorphic	95.8%

Installation and administration of *NetShield for NetWare* can be performed either directly from the server console, or more easily from the workstation using the *NetShield Console*. Loading of the console is password-protected, avoiding unwanted changes to the scanner's configuration. The password protection is perhaps somewhat over-eager, since immediately after installation access is prevented. Fortunately the default password is 'NetShield' which was guessed by the reviewer after a few attempts.

This is the first appearance of the *NetWare* product in *VB* tests since the swallowing of *Dr Solomon's* by *Network Associates*. The awkward interface that was reported previously has certainly been remedied during this takeover. Out of all the *Windows*-based administration consoles featured in this review, the *NetShield Console* proved to be the most straightforward and efficient to use.

An extremely limited file extension list proved once again to be *NetShield's* downfall. With viruses currently in the wild capable of infecting SCR and a range of *Office* files, such extensions simply have to be included in the default list. Rescanning in All Files mode showed the expected improvements, although *PowerPoint* samples infected with O97M/Tristate.C were still missed from the ItW test-set. In addition to the ACG samples, a handful of Marburg samples in the Polymorphic test-set were also missed.

Norman FireBreak v3.97 (30/04/99)

ItW File	98.8%	Macro	98.5%
ItW File (o/a)	98.8%	Macro (o/a)	98.5%
Standard	99.9%	Polymorphic	96.8%

Another product of uncertain identity, *FireBreak* (or is it *Virus Control*?) from *Norman Data Defense Systems* once again put in a strong performance across the *VB* test-sets.

Detection of the in the wild viruses was not up to the usual *Norman* standard, with two viruses slipping through the net. Firstly, as with most of the other products in this review, O97M/Tristate.C-infected *PowerPoint* samples were missed, despite the fact that PPT and POT files are included in the default extension list. In addition to this, misses were registered against Raadioga.1000 samples, a virus that has successfully been detected by *Norman* products in previous *VB* comparatives. Consultation with the product developers identified the problem and it has since been fixed.

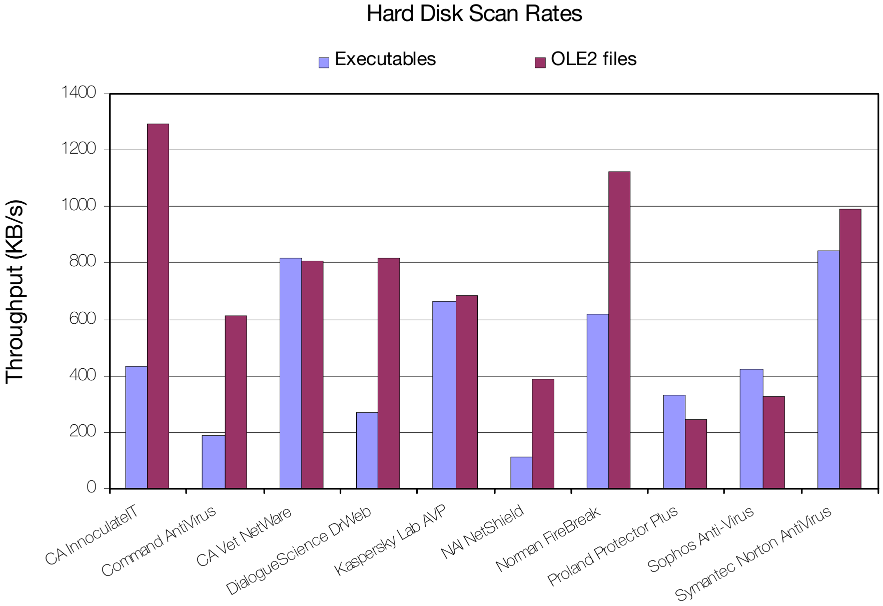
Administration of *FireBreak* is a simple, no-frills affair, performed entirely from the server console. Centralized surveillance and reporting can be enabled in a multiple server environment, by designating one server to be a communications hub.

Proland Protector Plus v6.6.A.01

ItW File	89.4%	Macro	42.5%
ItW File (o/a)	n/t	Macro (o/a)	n/t
Standard	32.4%	Polymorphic	22.3%

A regular entrant to *VB* Comparatives Reviews on other platforms, this is the first appearance of the *NetWare* version of *Protector Plus* from the Indian anti-virus company *Proland Software*.

Upon finding infected files, *PPN* attempts to cure them by default. Suprisingly, this option can neither be changed nor disabled – something that needs to be addressed. A further hinderance in testing the product is connected with the log files that are produced. A separate log is produced for each directory scanned, and deposited within that directory. Beside the fact that trawling through deep directory structures for log files is undesirable, a centralized log containing all infection reports would be far more sensible.



On the positive side however, achieving a detection rate of 89.4% against the ItW viruses is indicative of good progress by *Proland*, and their highest rating thus far in *VB* Comparative Reviews.

Sophos Anti-Virus v3.21

ItW File	99.7%	Macro	98.6%
ItW File (o/a)	99.7%	Macro (o/a)	98.6%
Standard	99.5%	Polymorphic	96.8%

As mentioned in the last *NetWare* comparative, installation of *Sophos Anti-Virus* (*SAV*) is achieved by copying a single NLM to the server manually, and then loading it.

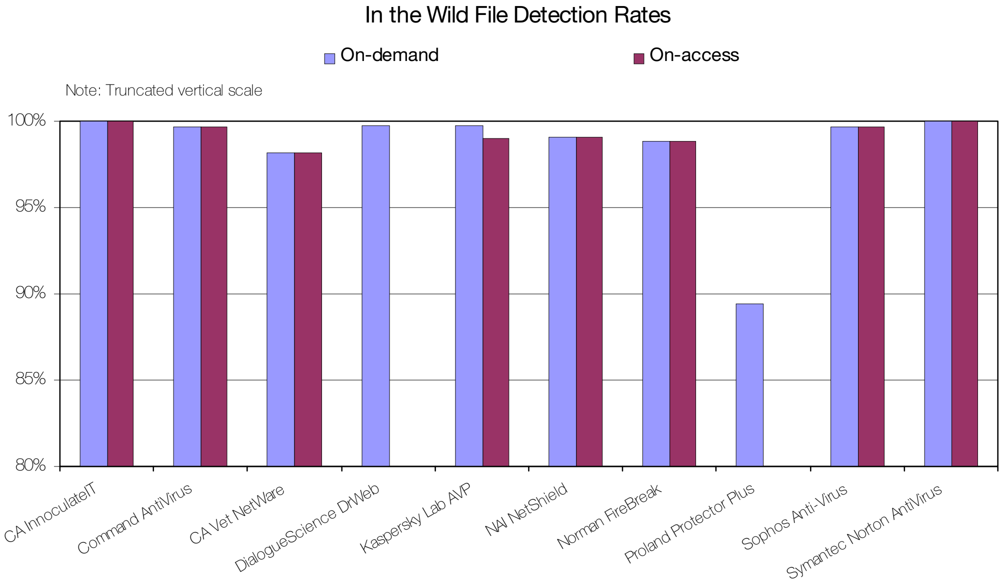
For the first time since March 1998, *Sophos Anti-Virus* failed to detect all the ItW viruses. *PowerPoint* and extensionless *Excel* samples infected with (yes, you guessed it!) O97M/Triplicate.C were missed during both on-demand and on-access scanning. Repeating the tests scanning All Files with *SAV's* default 'Quick' scan (compared to the more thorough 'Full' scan) resulted in detection of the extensionless *Excel* sample, but not the elusive *PowerPoint* samples.

In order to make the results more comparable with those obtained using other products, the results quoted for on-access detection are those obtained using the real-time monitor that is provided with *SAV*. The familiar *Intercheck* component was not tested. One notable point is that the scanning speeds reported in this review are those for the first scan, in which *InterCheck* checksums are created. Subsequent scans were performed at almost twice the rate (for the executable set).

Symantec NAV v4.04

ItW File	100.0%	Macro	99.4%
ItW File (o/a)	100.0%	Macro (o/a)	99.4%
Standard	100.0%	Polymorphic	96.8%

Having dropped its guard against Win95/Fono during the *Windows 98* comparative, *Norton AntiVirus* (*NAV*) brings up the rear in style this month – the only product managing to detect the full complement of in-the-wild viruses thrown at it.



	On-Access Scanner Overhead				Hard Disk Scanning Speed					
					Executables			OLE2 files		
	Loaded Inactive	Read or Outgoing	Write or Incoming	Read and Write	Time (min:sec)	Throughput (kB/s)	FPs [susp]	Time (min:sec)	Throughput (kB/s)	FPs [susp]
CA InnoculateIT	1.4%	15.5%	46.6%	42.5%	21:02	433.4	0	0:53	1292.5	0
Command AntiVirus	-1.9%	-2.6%	46.8%	49.4%	48:37	187.5	0	1:52	611.6	0
CA Vet NetWare	-2.4%	39.1%	17.1%	90.2%	11:10	816.3	1	1:25	805.9	0
DialogueScience DrWeb	n/t	n/t	n/t	n/t	33:30	272.1	[19]	1:24	815.5	[1]
Kaspersky Lab AVP	4.9%	200.0%	2.9%	410.0%	13:44	663.8	0	1:40	685.0	0
NAI NetShield	7.0%	14.9%	76.1%	78.7%	81:00	112.5	0	2:56	389.2	0
Norman FireBreak	-2.2%	95.0%	54.6%	146.9%	14:45	618.0	0	1:01	1123.0	0
Proland Protector Plus	n/a	n/a	n/a	n/a	27:19	333.7	5	4:38	246.4	1
Sophos Anti-Virus	-2.6%	n/a	52.9%	25.5%	21:32	423.3	0	3:30	326.2	0
Symantec Norton AntiVirus	-0.8%	28.6%	30.3%	63.8%	10:47	845.3	0	1:09	992.8	0

In common with the bulk of the products reviewed, installation of *NAV* is performed from the workstation. Configuration of the scanner is achieved using the *Windows*-based configuration utility on the workstation. Once configured, initiation of an on-demand scan can be achieved from either the workstation or the server console. Passwords can be used to prevent anyone other than the Administrator loading the main *NAVNLM* module, altering the program configurations or disabling real-time protection and scheduled scans.

Summary and Conclusions

It is encouraging to see most of the products achieving high detection rates across the bulk of the test-sets. However, the fact that only two out of ten products managed to detect 100% of the In the Wild test-set samples may perhaps alarm some readers.

By altering product configurations, detection of some of the missed samples across the Macro and ItW test-sets was achieved. Are the misses definitive therefore? Well, to be honest, yes. With reference to the missed O97M/Tristate.C-infected *PowerPoint* samples, the issue of file types is somewhat immaterial (the only additional product that would have detected 100% of the samples if the tests were run in 'All Files' mode was *DrWeb*).

Even if this were not the case, the simple fact is that the products should be continually developed to protect users from viruses they are most at threat from – i.e. those viruses that are in-the-wild. Some of the products – 'designed to provide optimum protection' – actually advise users not to adjust the default configurations.

With regards to the missed O97M/Tristate.C samples, all the products detected the infected *Word* and *Excel* files successfully. So, despite infected *PowerPoint* files remaining undetected, the products *will* detect the continual reinfection of the *Word* and *Excel* environments. The ensuing telephone calls to Technical Support would then no doubt resolve the problem. This is not sufficient protection, however. Examination of how the products performed against other non-ItW *PowerPoint* viruses shows the problem to be due to the inability of the majority of products to deal successfully with files of *PowerPoint* format. At the time of testing, only two of the products featured here (the *iRiS* engine-powered *InnoculateIT* and *Symantec's Norton Anti-Virus*) managed to detect such samples successfully.

So, is it disconcerting that eight out of ten products did not detect all the ItW viruses? Perhaps so, but not that surprising. However, from the discussions *VB* has had with the product developers it would appear that *current* versions of those products have learned how to scan *PowerPoint* file formats. With the submission deadline for the next comparative looming, whether or not this is true will soon become apparent.

Technical Details

Test Environment: Server – *Compaq Prolinea 590*, 90MHz Pentium with 80 MB of RAM, 1 GB hard disk, running *NetWare 4.10*, with 410PT8B, LIBUPI, DS410N and STRTL7 applied. Workstation – 166 MHz Pentium with 4 GB HD, CD-ROM and 3.5-inch floppy, running *Windows 98* with *Novell's Client 32*.

Virus Test-sets: Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/NetWare/199907/test_sets.html.

A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.